

# Technical Note TN-3255-SR

## TB9100 / Console Gateway / P25 TAG

### Version 4.10 Release Note

29 March 2022

This technical note contains information to accompany version 4.10 of the TB9100 base station, P25 console gateway and P25 trunked analog gateway (TAG) firmware. This is a commercial release and supports both trunked and conventional operation in base stations, and both trunked and conventional gateways.

## CONTENTS

1	WHAT'S NEW IN THIS RELEASE .....	3
1.1	What's New in Security .....	3
1.1.1	Updated SSH server .....	3
1.1.2	Firmware files are signed .....	3
2	KNOWN PROBLEMS OR LIMITATIONS .....	4
2.1	TM Tx Key does not include any signalling from the selected Signalling Profile .....	4
2.2	CSS: Crash with "Unexpected Error" .....	4
2.3	Alarms: Low forward power alarm does not clear .....	4
2.4	Alarms: Custom alarms may not generate SNMP traps .....	5
2.5	Base station: connectivity loss (rare) .....	5
2.6	Base station: Digital board DSP resets (rare) .....	5
2.7	Base station: Revert to Run mode changes not immediate .....	5
2.8	Base station: Call statistics count P25 voice call twice .....	5
2.9	Base station: Repeated contention between dispatcher and radio can cause a reset (rare) .....	5
2.10	Base station: Removing external reference causes reset .....	6
2.11	CSS: BER meter only works with configured NAC .....	6
2.12	CSS: Custom alarms are green, not red .....	6
2.13	CSS: Call statistics inaccurate for calls from analog line .....	6
2.14	DFSI: Cannot hear or talk to analog line .....	6
2.15	PMU: DC-powered PMUs can fail after a firmware upgrade .....	6
2.16	Trunked analog gateway: RFSS system calls not supported .....	7
2.17	Trunked analog gateway: Radio Unit Monitor feature does not comply with TIA standard .....	7
2.18	Analog line: Call setup time too long .....	7
2.19	Base station stops repeating when disconnected from the network .....	7

2.20	Base station: Conventional simulcast with tail timers not working.....	8
2.21	Data gateway: No indication on startup when mobile IP router is unavailable .....	8
2.22	Network: Channel bandwidth requirements increased.....	8
2.23	RF linking: Call statistics may not update .....	8
2.24	RF linking: Loopback and channel access problems .....	8
3	COMPATIBILITY.....	9
4	UPDATING CSS V4.09 WITH V4.10 FIRMWARE .....	11
5	FIRMWARE UPGRADE.....	12
5.1	PMU Hardware V1.01 Firmware Limitations.....	13
6	PUBLICATION INFORMATION .....	14

## 1 WHAT'S NEW IN THIS RELEASE

Release 4.10 provides updated base station and gateway software only, no corresponding CSS. CSS version 4.09 is still the current CSS release.

Release 4.10 provides one change only, an updated SSH server. See section 5 for firmware upgrade details.

### 1.1 What's New in Security

#### 1.1.1 Updated SSH server

Dropbear is the SSH server component that is used on the TB9100.

The previous SSH server utilised is version *0.49 - Fri 23 February 2007*.

For this release the SSH server has been updated to the latest current release *2020.81 - 29 October 2020*. This patches several security vulnerabilities.

For details on the changes, and issues addressed please see;

<https://matt.ucc.asn.au/dropbear/CHANGES>

To update the SSH server a TFTP upgrade is required, please see "TN-977c Upgrading Firmware using TFTP".

The version can be checked after upgrade by connecting to the TB9100 using SSH and typing "dropbear -V". The version reported should be "**Dropbear v2020.81**"

#### 1.1.2 Firmware files are signed

This release provides gateway and base station firmware only, as self-extracting executables.

These files have been signed by Tait. This can be verified (in windows 10) by right clicking on the file and choosing "Properties".

A digital signatures Tab should exist, and the name of the signer should be listed as "Tait International Limited"

## 2 KNOWN PROBLEMS OR LIMITATIONS

The following are known problems or limitations of version 4.10 of the TB9100 base station, the P25 console gateway, and the P25 trunked analog gateway.

### 2.1 TM Tx Key does not include any signalling from the selected Signalling Profile

Selecting TM Tx Key in the task manager will key the transmitter but not include any NAC or subaudible signalling to be transmitted. The help indicates that signalling will be included. This applies to V4.00 and all previous versions where TM Tx Key is supported.

### 2.2 CSS: Crash with “Unexpected Error”

The CSS may crash with “Unexpected Error” when viewing a page with a list control, for example, when viewing Monitoring>Data Logging>Call Record Log. The crash occurs because of an incompatibility between a Microsoft list control and newer operating systems. If it occurs please download and install the hotfix from Microsoft:

<https://support.microsoft.com/en-us/kb/896559>.

### 2.3 Alarms: Low forward power alarm does not clear

A low forward power alarm, once raised, may never clear in some cases. The alarm can be caused by momentary problems such as ice or a roosting bird on the antenna.

The alarm clears automatically in conventional systems and in trunked simulcast systems if the base station is a satellite voter. The alarm does not clear in all base stations within non-simulcast trunking systems and in master base stations within simulcast trunking systems.

The situation occurs as follows. Once the alarm is raised, the site controller takes the base station out of service. The alarm can only be cleared when the base station transmits without low forward power. This never happens, because the base station is out of service.  
(TIMS00072737)

*Work-around:* Add the following to the Task Manager of trunked base stations.

Flag	PA_AlmActive
Timer	PA Alm Timer max 30s
Custom input	PA Alm Cust In: Timer expired (PA Alm Timer) AND Flag (PA_AlmActive)
Custom actions	CustomAction1: SetFlag (PA_AlmActive);StartTimer (PA Alm Timer) CustomAction2: TransmitCWIDNow;StartTimer (PA Alm Timer)
Tasks	IF PA Alarm ON THEN CustomAction1 IF PA Alm Cust In THEN CustomAction2 IF NOT PA alarm on THEN Clear Flag (PA_AlmActive)

## 2.4 Alarms: Custom alarms may not generate SNMP traps

Custom alarms can be set up to trigger on a change in a digital input line, but may not generate an SNMP trap when the alarm is triggered. This is because the Enterprises.16304 MIB has a single trap for all custom alarms. If one custom alarm is active, another custom alarm will not generate another SNMP trap. (TIMS00093869)

## 2.5 Base station: connectivity loss (rare)

On start up or firmware download, there is a small chance that the base station loses connectivity with the CSS. This is caused by the reciter digital board failing to start properly.

*Workaround:* Travel to the base station and manually power cycle it. Consider installing IP-controlled power rails, which enable you to remotely turn AC power off and on again. (TIMS00096435)

## 2.6 Base station: Digital board DSP resets (rare)

In some base stations, the digital board DSP resets from time to time. If this occurs during a voice call, it causes a brief loss of voice, similar to a fade. When the DSP resets for the fifth time, the whole base station resets, interrupting service for at least 10 seconds.

## 2.7 Base station: Revert to Run mode changes not immediate

Users can configure the base station to automatically revert from Standby mode to Run mode. However, the configuration change is only implemented when the base station goes into Run mode. Users must not change this configuration and then leave the base station in Standby mode, assuming that it will automatically revert.

*Workaround:* After changing the Revert to Run mode setting from Never to 2 minutes or 10 minutes, put the base station in Run mode manually. Thereafter, if the base station is left in Standby mode, it will automatically revert to Run mode. (TIMS00103421)

## 2.8 Base station: Call statistics count P25 voice call twice

When an SU makes a call, the call statistics (Monitor > Data Logging > Call Statistics) count the call twice; once when PTT is pressed, and once when it is released. (TIMS00081765, TIMS00083308)

## 2.9 Base station: Repeated contention between dispatcher and radio can cause a reset (rare)

Bench testing has discovered that a rapid succession of short calls (four or more with duration of less than one second) from both an analog FM user and a dispatcher connected to the base station's analog line can cause the base station to temporarily enter a stuck state. In extreme cases, the base station resets itself. Otherwise, it recovers within 40 seconds. If the CSS is connected to the base station during these events, the PA keyed LED

in the RF Interface monitoring form stays on even when the PA is not transmitting. After a while, the base station disconnects the CSS.

This issue does not affect Tait gateways.

While this problem is unlikely to occur in operational networks, network administrators should consider advising analog FM users to avoid repeated pressing of PTT when attempting to gain channel access, if the base station's analog line is used. (TIMS00078219)

## **2.10 Base station: Removing external reference causes reset**

Removing the base station's external reference can cause a DSP process to fail, causing the watchdog circuitry to reset the base station. Normal functioning is restored, but takes at least 30 seconds. (TIMS00064565)

## **2.11 CSS: BER meter only works with configured NAC**

The CSS displays the BER of a received signal in the Monitor > Interfaces > RF Interface form. If the received NAC is different from the configured NAC, the base station cannot measure the BER and the CSS displays a BER of 0.0000%. (TIMS00071380)

## **2.12 CSS: Custom alarms are green, not red**

When a custom alarm is triggered, its LED in the Custom Alarms page (Monitor > Task Manager > Custom Alarms) goes green instead of the expected red. (TIMS00093242)

## **2.13 CSS: Call statistics inaccurate for calls from analog line**

The Call Statistics form displays inaccurate values for the number of calls made, if calls were made from the analog line of the connected network element. The number of calls is correctly recorded in the call records log, in syslog messages, and in the CSS display when the CSS is connected to other channel group members. (TIMS00061018)

## **2.14 DFSI: Cannot hear or talk to analog line**

If one dispatch position is connected to the DFSI and another to the analog line of the same base station or P25 console gateway, the dispatchers will be able to communicate with SU users on the channel, but not with each other. The DFSI cannot hear the analog line and vice versa.

This is a side-effect of the design, which flags audio with the receiver number of the originating base station or gateway. Audio that has the receiver number of the base station or gateway is blocked from going out over the line. This stops dispatch audio looping back to the dispatcher. (TIMS00063909)

## **2.15 PMU: DC-powered PMUs can fail after a firmware upgrade**

There is a risk that DC-powered PMUs with serial numbers prior to 18076561 will fail to power up after a firmware upgrade. There is no risk for subracks with a single reciter and a

relatively low risk for a subrack with two reciters and two PAs. An active auxiliary power supply and the presence of multiple reciters both make the failure more likely. Newer PMUs have a small hardware change that resolves this issue. (TIMS00075032)

*Work-around:* The following options are available for older PMUs that are subject to this risk.

1. If the PMU can be AC-powered, make sure that it is running on AC before carrying out a remote firmware upgrade.
2. If the PMU can only run on DC and the firmware upgrade is necessary, carry it out on site. Before upgrading, unplug the auxiliary supply and any reciters other than No 1 (the one that configures the PMU).
3. If the PMU failed during an upgrade, restart it using the instructions in TN-1458. Alternatively, send it to an accredited service center.
4. To prevent the failure, you can carry out the required hardware change (see TN-1458).

## 2.16 Trunked analog gateway: RFSS system calls not supported

System calls to a particular RFSS (an Airbus core network feature using IDs other than 65535) cannot be initiated or joined by the trunked analog gateway. (TIMS00089213)

## 2.17 Trunked analog gateway: Radio Unit Monitor feature does not comply with TIA standard

The TIA standard specifies a silent mode bit. When the gateway sends a Radio Unit Monitor message, it should use this bit to tell the radio whether to operate stealthily (no UI indication) or not (Tx LED is lit up and display shows "Calling Dispatch").

The gateway leaves this bit at zero and cannot be configured to set it to 1. Radios following the older TIA standard will respond stealthily but those following the current standard (such as Tait radios with version 7.75.00.9119 onwards) will display the above indications. (TIMS00096930)

**Important: Because of the above issue, Tait radios may stop operating stealthily in response to the dispatcher's Radio Unit Monitor message, following a radio firmware upgrade.**

## 2.18 Analog line: Call setup time too long

The setup time for digital P25 calls by the dispatcher which use MDC1200 signaling over the analog line can be up to 750 ms, which can cause late entry by the receiving radio(s). Around 200 ms of this is delay within the analog console itself. Clearing the supplementary services check box reduces the delay by around 300 ms, at the cost of disabling the decoding of MDC1200 signaling for supplementary services. (TIMS00085529)

## 2.19 Base station stops repeating when disconnected from the network

If the Ethernet connection to the base station is disconnected, the base station continues local repeating until its IP buffer becomes full (Syslog messages continue to be sent). Then it

will stop repeating until the Ethernet connection is re-established and the IP buffer is cleared.  
(TIMS00091132)

## 2.20 Base station: Conventional simulcast with tail timers not working

Tail timers cannot be used with conventional simulcast because it causes problems with the traffic buffers. (TIMS00091535)

## 2.21 Data gateway: No indication on startup when mobile IP router is unavailable

If the home agent is unavailable or the data gateway is given an invalid home agent IP address, the CSS gives no indication of this, until radios have made 10 registration attempts. The MIP interface box (Monitor > Interfaces > Packet Data, State tab) changes its display from “Operational” to “HA no response.” In other words, the data gateway does not check that it is connected to the mobile IP router before declaring itself to be operational.  
(TIMS00085170)

## 2.22 Network: Channel bandwidth requirements increased

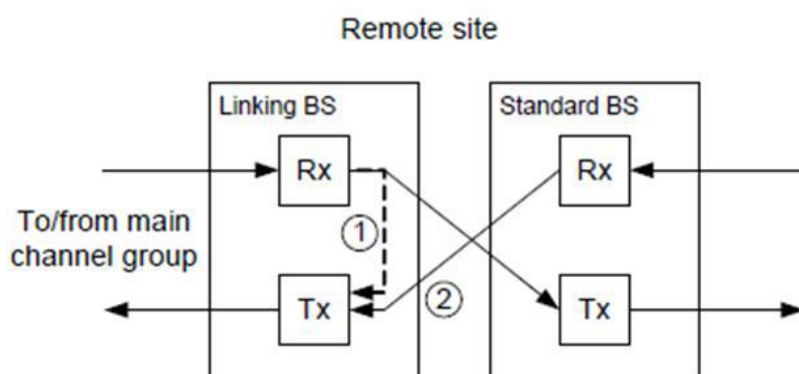
The base station, P25 console gateway, and trunked analog gateway now require 40 kbps bandwidth for their IP link. The increase is needed because RTP header compression is no longer applied. See the system manual for the current bandwidth requirements.  
(TIMS00073972)

## 2.23 RF linking: Call statistics may not update

A linking transceiver may not update the statistics for the number of calls, for example when RF calls are being received across the link. All other network elements provide correct call statistics. (TIMS00061023)

## 2.24 RF linking: Loopback and channel access problems

Testing has uncovered the following problems with RF linking.



1. Although the linking base station at the remote site is configured as a linking transceiver and the Allow loopback check box is cleared, loopback can still occur sometimes, as shown in the above diagram 1. This happens at the end of a call from a radio at the remote site and may result, depending on configuration, in an endless loop. Another call or putting the base station in standby ends the loop.
2. If the remote site is stressed by several quick PTT presses in succession, the linking base station may not transmit the call back to the main channel group (2 in the above diagram). (TIMS00077806). Workaround: Contact Tait for assistance.

### 3 COMPATIBILITY

The following table specifies all compatible configurations for the base station and for the gateways. A configuration is compatible if module firmware, module hardware, the CSS, and the calibration software have compatible versions. If changes are made to hardware or firmware, you need to check whether the new versions are compatible.

- Each row in the table identifies a compatible configuration.
- Each cell within a row contains the hardware, firmware, or software version number that is compatible with the other versions in the row. If a cell contains more than one version number, more than one version is compatible.
- Table footnote indicate any restrictions imposed on a particular combination by the hardware, firmware, or CSS version.
- Any other combination is **not** compatible and not supported.

TB9100	Calibration software	CSS	Data-base	MIBs	Network Board			Digital Board		PMU		PA	
					F/w	Kernel	H/w	F/w	H/w	F/w	H/w	F/w	H/w
4.10	3.09	4.09	3.92	3.96	4.05	3.60.06	00.01	3.98	00.07 <sup>1</sup> 00.06 00.05 <sup>2</sup> 00.04 00.03	3.16	01.01 01.00 00.03 00.02 00.01	3.14	01.00 00.02 <sup>3</sup> 00.01
4.09	3.09	4.09	3.92	3.96	4.02	3.60.06	00.01	3.98	00.07 <sup>4</sup> 00.06 00.05 <sup>5</sup> 00.04 00.03	3.16	01.01 01.00 00.03 00.02 00.01	3.14	01.00 00.02 <sup>6</sup> 00.01
4.02	3.09	4.00	3.92	3.96	4.02	3.60.06	00.01	3.97	00.07 <sup>1</sup> 00.06 00.05 <sup>2</sup> 00.04 00.03	3.16	01.00 00.03 00.02 00.01	3.14	01.00 00.02 <sup>3</sup> 00.01
4.00	3.09	4.00	3.92	3.96	4.00	3.60.06	00.01	3.97	00.07 <sup>1</sup> 00.06 00.05 <sup>4</sup> 00.04 00.03	3.16	01.00 00.03 00.02 00.01	3.14	01.00 00.02 <sup>3</sup> 00.01
3.97	3.09	3.97	3.92	3.96	3.97	3.60.06	00.01	3.97	00.07 <sup>1</sup> 00.06 00.05 <sup>2</sup> 00.04 00.03	3.16	01.00 00.03 00.02 00.01	3.14	01.00 00.02 <sup>3</sup> 00.01
3.96	3.09	3.96	3.92	3.96	3.96	3.60.05	00.01	3.96	00.07 <sup>1</sup> 00.06 00.05 <sup>2</sup> 00.04 00.03	3.16	01.00 00.03 00.02 00.01	3.14	01.00 00.02 <sup>3</sup> 00.01

<sup>1</sup>The digital board hardware version 00.07 supports simulcast operation. Earlier hardware versions are compatible with the indicated firmware version but cannot be used in simulcast systems.

<sup>2</sup>The digital board version 0.05 has a different exciter synthesizer circuit. Firmware v 2.1x and later can use the old or the new circuit.

<sup>3</sup>Version 00.02 extends the PA frequency range from 400–520 MHz to 380–520 MHz. This version must be used with H4 band reciters that will operate in the 380–400 MHz range

<sup>4</sup>The digital board hardware version 00.07 supports simulcast operation. Earlier hardware versions are compatible with the indicated firmware version but cannot be used in simulcast systems.

<sup>5</sup>The digital board version 0.05 has a different exciter synthesizer circuit. Firmware v 2.1x and later can use the old or the new circuit.

<sup>6</sup>Version 00.02 extends the PA frequency range from 400–520 MHz to 380–520 MHz. This version must be used with H4 band reciters that will operate in the 380–400 MHz range

TB9100	Calibration software	CSS	Data-base	MIBs	Network Board			Digital Board		PMU		PA	
					F/w	Kernel	H/w	F/w	H/w	F/w	H/w	F/w	H/w
3.95	3.09	3.95	3.92	3.91	3.95	3.60	00.01	3.95	00.07 <sup>1</sup> 00.06 00.05 <sup>2</sup> 00.04 00.03	3.16	01.00 00.03 00.02 00.01	3.14	01.00 00.02 <sup>3</sup> 00.01
3.91	3.08	3.91	3.91	3.91	3.91	3.60	00.01	3.91	00.07 <sup>1</sup> 00.06 00.05 <sup>2</sup> 00.04 00.03	3.16	01.00 00.03 00.02 00.01	3.14	01.00 00.02 <sup>3</sup> 00.01

## 4 UPDATING CSS V4.09 WITH V4.10 FIRMWARE

Install CSS V4.09 if you have not already done so.

There are 2 signed self-extracting archives with the V4.10 firmware available.

- firmware-bs.exe
- firmware-gw.exe

If you have a crypto cable reciter or gateway with a PAC0 suffix, use the firmware-gw, otherwise use the firmware-bs archive.

Double-clicking on the firmware-bs.exe or firmware-gw.exe will open a dialogue box with the current location of the files. If you want to extract the files here, click Extract, if not, enter the location to use.

Use this table to copy the files to the correct locations to upgrade the CSS

File	Copied to (CSS default location)	Comments
QBA10PAA03.14	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files	This file already exists in CSS 4.09.
QBA10PMA03.16	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files	This file already exists in CSS 4.09.
QBA20ASU040500	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files	
QBA20REA039800	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files	
QBA20ASE038104	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files	Crypto capable reciters and gateways only.
TB9100FC041000.csv	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files	

These files are copied to the TFTP Download folder.

File	Copied to (CSS default location	Comments
QBA20ASA040500	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files\TFTP Download	
QBA20ASK036006	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files\TFTP Download	
testfile	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files\TFTP Download	Overwrite the existing file
upscript	C:\Program Files (x86)\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files\TFTP Download	Overwrite the existing file

## 5 FIRMWARE UPGRADE

**Note:** Read the reciter configuration before performing the upgrade.

A base station firmware upgrade from V4.09 or earlier must be performed using TFTP for the new SSH server to be installed. Please see “*TN-977c Upgrading Firmware using TFTP*” for more information.

Before the upgrade, the SSH login returns this information

```
BusyBox v1.00 (2016.01.06-01:29+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
# dropbear -v
Unknown argument -v
Dropbear sshd v0.49
```

After the upgrade, the version of Dropbear is v2020.81

```
BusyBox v1.00 (2022.02.09-02:08+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
# dropbear -V
Dropbear v2020.81
```

When completed, reconnect with the CSS. A channel module “Network board configuration alarm” is likely to be active in Monitor > Alarms > Status. Program the reciter with the configuration read before the upgrade and the alarm will be cleared.

To check the active version of firmware, go to Monitor > Module Details > Channel Module. The Network element and Network board firmware versions will display 04.05

Versions		
Network element:	04.05	
	Digital board	Network board
Serial number:	18084642	2239213
Firmware:	03.98	04.05
Kernel version:		03.60
Hardware:	00.07	00.01
Database:		03.97

## 5.1 PMU Hardware V1.01 Firmware Limitations

The PMU microprocessor has new firmware identifying itself as V3.16 to the TB9100 reciter. This PMU firmware cannot be upgraded or downgraded via the CSS. V3.16 PMU firmware is compatible with previous base station versions back to V3.81 released July 2013.

If an old PMU is being replaced with a new PMU with hardware V1.01 in a base station running firmware earlier than V3.81 and the base station firmware cannot be upgraded to V3.81 or later, contact Tait Technical Support.

## 6 PUBLICATION INFORMATION

<b>Related Documentation</b>	Customer Service Software User's Manual MBA-00003-21 · Issue 21 · July 2016			
<b>Compliance Issues</b>	None.			
<b>Compatibility Issues</b>	PMU hardware V1.01 does not support reciter firmware earlier than V3.81.			
<b>CSO Instruction</b>	None			
<b>Confidentiality</b>	<p>Confidential – This message or document contains proprietary information intended only for the person(s) or organisation(s) to whom it is addressed.</p> <p>All recipients are legally obliged to not disclose Tait technological or business information to any persons or organisations without the written permission of Tait.</p>			
<b>Distribution Level</b>	Channel partners			
<b>Document History</b>	<b>Issue</b>	<b>Date</b>	<b>Description</b>	<b>Author</b>
		29 March 2022	First release	J Northcott